PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00, 3/16 — A1

(11) International Publication Number: WO 00/07087

(43) International Publication Date: 10 February 2000 (10.02.00)

(21) International Application Number: PCT/US99/16880

(22) International Filing Date: 27 July 1999 (27.07.99)

(30) Priority Data:

60/094,168	27 July 1998 (27.07.98)	US
60/094,169	27 July 1998 (27.07.98)	US
60/094,260	27 July 1998 (27.07.98)	US

(71) Applicant *(for all designated States except US)*: VERITEL CORPORATION [US/US]; Suite 710, 70 West Madison, Chicago, IL 60602 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: TOMES, Christopher [US/US]; Apartment 6DE, 312 N. May, Chicago, IL 60607 (US). ENGLESTAD, Greg [US/US]; Apartment 4, 4070 Riviera Drive, San Diego, CA 92109 (US).

(74) Agents: CARLSON, Stephen, C. et al.; McDermott, Will & Emery, 600 13th Street, N.W., Washington, DC 20005 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(54) Title: SYSTEM OF ACCESSING CRYPTED DATA USING USER AUTHENTICATION

(57) Abstract

User authentication is performed by verifying that a voice sample of a user belongs to an enrolled user, with an alternative access means of asking a series of personal questions. Access to computer resources such as files and applications are controlled by a voice verification file management program that encrypts files and applications selected by an authenticated user. A vault is also provided, in which even the names of the files and applications placed in the vault are scrambled.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SYSTEM OF ACCESSING CRYPTED DATA USING USER AUTHENTICATION

RELATED APPLICATIONS

The present application claims the benefit of U.S. Provisional Application No. 60/094,168 entitled "SYSTEM AND METHOD FOR VOICE VERIFICATION" filed on July 27, 1998 by Christopher Tomes, U.S. Provisional Application No. 60/094,169 entitled "MULTIMEDIA VOICE VERIFICATION SYSTEM AND METHOD FOR" filed on July 27, 1998 by Christopher Tomes, and U.S. Provisional Application No. 60/094,260 entitled "SYSTEM AND METHOD FOR VOICE VERIFICATION" filed on July 27, 1998 by Christopher Tomes and Greg Engelstad, the contents of each of which are hereby incorporated by reference herein.

FIELD OF THE INVENTION

The present invention relates to computer security and more particularly to a system and method for user authentication.

BACKGROUND OF THE INVENTION

Determining who is an authorized user of a computer resource such as a file, a program, or even an entire computer system, is a very important aspect of computer security. "User authentication" refers to the process of validating a user to verify that the user is not a counterfeit.

The most common form of user authentication is by login and password, in which the user is presented with a password prompt that asks the user to input a password via the keyboard. The text of the password is typically encrypted and compared against an encrypted enrolled password in an enter for the login in a database. If the encrypted entered password matches the encrypted enrolled password, then the person entering the login and password is considered authenticated.

Such key-based passwords, however, have a number of disadvantages that compromise security. For example, security can be affected if users employ easily guessed passwords such as their name, address, and birth date. Other easily guessed passwords include popular makes of cars such as "Ferrari" and popular television shows. Since key-based passwords are entered by the keyboard, it is relatively simple to impersonate an

authorized user if the password is known or easily guessed. Every key stroke is identical from user to user.

Accordingly, system administrators have been recommending that users employ passwords that are difficult to guess, such as a word appended by arbitrary numbers or even randomly assigned passwords. A difficulty with hard to guess passwords is that they are hard to remember, so many users are tempted to write such passwords down. The security of a password that has been written down on paper is only as good as the physical security of the piece of paper. Despite frequent admonishment, a large number of users often attach their passwords to their computers and laptops with a sticky note.

Other attempts to authenticate users have been developed such as fingerprint scanning and retina scanning. These "biometric" approaches have so far required very sophisticated equipment and are therefore prohibitively expensive for the typical affordable computer system. Consequently, biometric security has truly only been available to the government and major corporations and out of the reach of the common computer owner.

What is needed is a way to authenticate a user than cannot be easily counterfeited, e.g. by guessing a user's self-selected key-based password, but is still easy to remember so that the user does not compromise security by writing the password down. There is also a need for an affordable user authentication system, in contrast to fingerprint and retina scanning, that does not have the disadvantages associated with key-based passwords.

SUMMARY OF THE INVENTION

These and other needs are addressed by the present invention, in which the password such as a user's name is spoken by the user. The present invention stems from the realization that a person's voice is unique and can be used to authenticate a user, even the user's password is known or easily guessed. Unlike fingerprint and retina scanning, voice verification can be readily implemented with low cost hardware, such as a microphone.

Affordable computer security is especially important for files stored on personal computers and laptops, where the physical access to the personal computer and laptop is difficult to control. Accordingly, one aspect of the present invention relates to a method and program for controlling access to a file by receiving an input voice sample from a user, verifying that the input voice sample belongs to an enrolled user, and decrypting the file based on the result of the verification. Thus, two techniques are used to secure a sensitive

file on a computer: voice verification, which protects the file against unauthorized use (by inauthentic users) and file encryption, which protects the file against unauthorized access.

Another aspect invention therefore involves a "vault," in which a collection of files and applications are managed by voice verification and file level encryption. In some cases, even the knowledge of the existence of a document on a computer or laptop is sensitive. In one embodiment, therefore, each such file is moved to a specified directory in the vault and given a scrambled name to make it very difficult for a computer user to identify the file by name without, of course, going through the voice verification process.

Other aspects of the invention pertain to using voice verification to launch a computer application and grant access to a computer system, thereby replacing the login and key-based password process. In fact, voice verification can be used at a private branch exchange to control access to the public switched telephone network, thereby reducing long-distance toll charges made by unauthorized individuals.

In one embodiment, voice verification is accomplished by an initial user enrollment phase, in which an authorized user utters several words into a microphone. These words can be chosen by the user, by the system, or both. The utterances are sampled, segmented into frames (typically corresponding to each phone in the utterance), and processed to produce a voice print. This voice print may constitute an array of Cepstral, linear predictive coding, or other coefficients for each frame. Preferably, several utterances of the same word are sampled and averaged, thereby allowing for a range of normal variation in the person's voice to be accepted.

During a subsequent verification phase, a user is prompted to utter the password, which is sampled, segmented, and processed to produce a voice print. The input voice print is compared with the enrolled voice print, and a dissimilarity measure is calculated. If the dissimilarity measure is less than a predefined threshold, then the user is considered verified. One feature is a slider bar that allows the user to set the security level by controlling the predefined threshold value.

Occasionally, the user's voice may be very hoarse due to a sickness such as laryngitis. Accordingly, an alternative access method is provided in some implementation by user profile questions. A user profile question is a question that asks for personal information of user that is difficult for someone other than the user to know but unforgettable to the user and does not need to be written down. Examples of user profile questions include, "What is your mother's maiden name?" and "What is the color of your

first car?" Another alternative access method is a "one-time password" that is generated by the voice verification program and can only be used a single time. Since the one-time password can only be used once, the security drawbacks with committing the one-time password to writing is greatly attenuated.

Still other objects and advantages of the present invention will become readily apparent from the following detailed description, simply by way of illustration of the best mode contemplated of carrying out the invention. As will be realized, the invention is capable of other and different embodiments and its several details are capable of modifications in various obvious respects, all without departing from the invention. Accordingly, the drawings and description are to be regarded as illustrative in nature, and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

FIG. 1 is a schematic diagram of computer system that can be used to implement an embodiment of the present invention.

FIG. 2 is a flowchart of enrolling an authorized user.

FIG. 3A illustrates a dialog box for taking voice samples.

FIG. 3B illustrates a dialog box for getting user profile questions and answers.

FIG. 4 is a flowchart of authenticating a user.

FIG. 5A illustrates a dialog box for getting a user name.

FIG. 5B illustrates a dialog box for getting a voice sample.

FIG. 5C illustrates a dialog box for getting user profile answers.

FIG. 5D illustrates a dialog box for getting a one-time password.

FIG. 6A illustrates a main application window.

FIG. 6B illustrates a menu for file operations.

FIG. 6C illustrates a dialog box for exporting an encrypted file.

FIG. 7 is a flowchart of securing access to a file.

FIG. 8 is a flowchart of releasing access to a file.

FIG. 9A illustrates a menu for user options.

FIG. 9B illustrates a dialog box for adjusting enrolled voice samples.

FIG. 9C illustrates a dialog box for displaying a one-time password.

DESCRIPTION OF THE PREFERRED EMBODIMENT

A method and system for controlling access to a resource by voice verification are described. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

HARDWARE OVERVIEW

Figure 1 is a block diagram that illustrates a computer system 100 upon which an embodiment of the invention may be implemented. Computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information. Computer system 100 also includes a main memory 106, such as a random access memory (RAM) or other dynamic storage device, coupled to bus 102 for storing information and instructions to be executed by processor 104. Main memory 106 also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor 104. Computer system 100 further includes a read only memory (ROM) 108 or other static storage device coupled to bus 102 for storing static information and instructions for processor 104. A storage device 110, such as a magnetic disk or optical disk, is provided and coupled to bus 102 for storing information and instructions.

Computer system 100 may be coupled via bus 102 to a display 112, such as a cathode ray tube (CRT), for displaying information to a computer user. An input device 114, including alphanumeric and other keys, is coupled to bus 102 for communicating information and command selections to processor 104. Another type of user input device is cursor control 116, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 104 and for controlling cursor movement on display 112. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), that allows the device to specify

positions in a plane. A microphone 117 is also provided for converting sounds and other acoustical signals into electric signals for processing by computer system 100.

The invention is related to the use of computer system 100 for controlling access to a resource by voice verification. According to one embodiment of the invention, controlling access to a resource by voice verification is provided by computer system 100 in response to processor 104 executing one or more sequences of one or more instructions contained in main memory 106. Such instructions may be read into main memory 106 from another computer-readable medium, such as storage device 110. Execution of the sequences of instructions contained in main memory 106 causes processor 104 to perform the process steps described herein. One or more processors in a multi-processing arrangement may also be employed to execute the sequences of instructions contained in main memory 106. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.

The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 104 for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical or magnetic disks, such as storage device 110. Volatile media include dynamic memory, such as main memory 106. Transmission media include coaxial cables, copper wire and fiber optics, including the wires that comprise bus 102. Transmission media can also take the form of acoustic or light waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, DVD, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor 104 for execution. For example, the instructions may initially be borne on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system 100 can receive the data

on the telephone line and use an infrared transmitter to convert the data to an infrared signal. An infrared detector coupled to bus 102 can receive the data carried in the infrared signal and place the data on bus 102. Bus 102 carries the data to main memory 106, from which processor 104 retrieves and executes the instructions. The instructions received by main memory 106 may optionally be stored on storage device 110 either before or after execution by processor 104.

Computer system 100 also includes a communication interface 118 coupled to bus 102. Communication interface 118 provides a two-way data communication coupling to a network link 120 that is connected to a local network 122. For example, communication interface 118 may be an integrated services digital network (ISDN) card or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface 118 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, communication interface 118 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

Network link 120 typically provides data communication through one or more networks to other data devices. For example, network link 120 may provide a connection through local network 122 to a host computer 124 or to data equipment operated by an Internet Service Provider (ISP) 126. ISP 126 in turn provides data communication services through the worldwide packet data communication network, now commonly referred to as the "Internet" 128. Local network 122 and Internet 128 both use electrical, electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 120 and through communication interface 118, which carry the digital data to and from computer system 100, are exemplary forms of carrier waves transporting the information.

Computer system 100 can send messages and receive data, including program code, through the network(s), network link 120, and communication interface 118. In the Internet example, a server 130 might transmit a requested code for an application program through Internet 128, ISP 126, local network 122 and communication interface 118. In accordance with the invention, one such downloaded application provides for controlling access to a resource by voice verification as described herein. The received code may be executed by processor 104 as it is received, and/or stored in storage device 110, or other non-volatile

storage for later execution. In this manner, computer system 100 may obtain application code in the form of a carrier wave.

USER ENROLLMENT

User enrollment is a preliminary procedure in which voice samples of an authorized user is obtained. These voice samples are preferably processed into a compact from referred to as voice prints, which is used for comparison against voice prints of those users desiring to obtain access to the system. User enrollment may occur, for example, as part of the installation of voice verification software.

Referring to FIG. 2, the "user name" of the user is obtained in step 202. The user name, which is a text string that can be the user's first name, last name, or user id, similar to a login name, serves to identify an authorized user. In one implementation illustrated in FIG. 3A, the user name is obtained by means of a text field 302 in a user definition dialog box 300. Referring back to FIG. 2 at step 204, the user is prompted (e.g. by an audio prompt) to speak a password into a microphone 117. This password can be any word the user chooses and is typically the user's name. At step 206, several voice samples of password is taken and a composite voice print is extracted from the samples.

Various techniques can be employed to extract a voice print from a voice sample, but the present invention is not limited to any particular technique. One possible technique involves buffering the incoming speech signal and processing the buffered speech signal in segments of 330 samples with overlaps of 220 samples. Each segment is then windowed using a Hamming window and an energy profile of the speech is obtained. Using the energy profile, the beginning and end point of an energy event is detected. An energy event, which is coincides with a new phone in the utterance, is defined as an occurrence of the energy exceeding a minimum threshold for a given number of frames. All energy events are indexed for further processing. Each frame corresponding to a detected energy event is processed to extract the voice print. Specifically, for each frame, the first ten autocorrelation coefficients are calculated and Levinson-Durbin recursion is applied to obtain a tenth order LPC (linear predictive coding) coefficient set. From the LPC coefficients, a tenth order Cepstrum is then calculated. Accordingly, the final voiceprint is formed as a set of the 10 Cepstral coefficients for each frame corresponding to a detect energy.

In addition to taking a voice print of a word of the user's choosing, voice prints for additional or supplemental words are taken in one embodiment. These words can be

predetermined by the voice enrollment/verification software, or they can be the answers to predetermined personal questions such as the user profile questions described hereinafter. Thus, in step 208, each supplemental word, e.g. four of them, are prompted for (as by an audio prompt), and, in step 210, voice samples are obtained and processed to extract corresponding voice prints.

It is recognized that a user's voice may become unavailable from time to time, for example, when the user becomes hoarse after too much talking or comes down with an illness such as laryngitis. In one embodiment therefore, an alternative access means is provided, wherein the user is prompted in step 212 to answer a number of personal, "user profile" questions. Any question that asks for information in the personal knowledge of an individual and which the individual is not likely to write down is a good candidate for a user profile question.

The dialog box 310 illustrated in FIG. 3B displays one list of possible user profile questions that includes, "What is your mother's maiden name?"; "Where was your father born?"; "Where was your mother born?"; "Where did you attend elementary school?"; "Where did you attend 7th grade?"; What is the color of your first car?"; "What is the make of your first car?"; and "What are the last four digits of your social security number?". At step 214, selections of which user profile questions to be used are made and their answers are obtained from the user.

If a plurality of users is supported, then the obtained voice prints and user profile answers are stored in association with the user name. Therefore, the user name serves to distinguish between different enrolled users.

As a third access means, a one-time password may be optionally generated in step 216. The one-time password can be implemented as a string of 16 random characters, which would only work once as a password. Even though the one-time password is likely to be written down, it is valid only once, unlike conventional passwords that are valid until explicitly changed, so that the security issues relating to the one-time password can be more easily controlled.

VOICE VERIFICATION

As soon as one or more users have been enrolled, the system is ready to control access to resources such as files and applications by requiring a user who desires the access the resources to undergo a voice verification procedure. In an exemplary voice verification

procedure shown in FIG. 4, the user name is obtained in step 402, for example, from a text field 502 in dialog box 500 illustrated in FIG. 5A. When the user presses the enter key, voice verification dialog box 510 of FIG. 5B is displayed, and the user is prompted in step 404 (as by an audio prompt) to give the password by speaking into the microphone 117.

In step 406, a voice sample of password spoken by the user is obtained, and the voice print is then extracted. In addition, at least one of the supplemental words is prompted for (step 408) and voice prints for the supplemental words are obtained. Dialog box 510 in FIG. 5B features a small color screen 512 that indicates a current state of the voice sampling and verification process, a button 514 for skipping the voice verification procedure and selecting the user profile question alternative authentication method, a button 515 for skipping the voice verification procedure and selecting the one-time password alternative authentication method, a button 516 for stopping the voice verification, and a close button 518 for quitting the voice verification process altogether.

At step 412, if the voice prints from the voice samples input in steps 406 and 410 match the corresponding voice prints, then the user is considered to be authenticated (step 414). Various techniques exists for matching an input voice print with an enrolled voice point, but the present invention is not limited to any particular technique. In one implementation, the voiceprint matching is performed by a dynamic time warping (DTW) algorithm that allows for a minimum slope of 0.5 and a maximum slope of 2.0. The shorter of the voiceprints to be matched is designated the "guide," and the other voiceprint is designated the "slave." Beginning and end point deviations, both on the guide and slave, are checked to see if they fall within about one-fifth the length of the slave signal. The distance at each point is calculated using a Euclidean measure of comparing a set of weighted coefficients from the slave with a set of weighted coefficients from the guide. Once all the distances are calculated, the path with a minimum sum of distances is determined and the cost per node of such path is returned as the dissimilarity measure. If the dissimilarity measure falls below a defined threshold, a match is determined to exist, resulting in a successful verification. Otherwise, the voice prints are considered unmatched with the result being an unsuccessful verification.

The alternative access method by user profile questions is employed when the voiceprints fail (from step 412) or when the user selects the "Use User Profile Questions" button 514 in the voice authentication dialog box 510. At step 416, the user profile questions dialog box 520 (in FIG. 5C) is displayed, prompting with one of the user profile

questions in text box 522. The user profile answer is entered into text field 524 in step 418. Preferably, steps 416 and 418 are repeated additional times, but with different user profile questions. If all of the questions match in step 420, then the user is authenticated (step 414). The user profile questions dialog box 520 also includes a use voice authorization button 525 to go back to step 404 and a use one-time password button 526 to go forward to step 422. The close button 528 exits the authentication procedure.

Still another access method by a one-time is employed when the user profile questions fail (from step 420) or when the user selects the "One Time Password" button 515 in the voice authentication dialog box 510 or the "One Time Password" button 525 in the user profile questions dialog box 520. At step 422, the one-time dialog box 530 (in FIG. 5D) is displayed, prompting for the one-time password in text box 532. The user one-time password is entered into text field 534 in step 424. If the one-time password matches in step 426, then the user is authenticated (step 414). Otherwise, the user is rejected in step 428. The one-time password dialog box 530 also includes a use user profile questions button 535 to go back to step 422 and a use voice authorization button 536 to go back to step 404. The close button 538 exits the authentication procedure.

The above-described voice verification procedure is capable of use in a variety of different applications as a general replacement for key based passwords. For example, such voice verification technology can be used for logging into a computer and/or server. In fact, a private branch exchange (PBX) at a company can use this technology for controlling access to the public switched telephone network (PSTN), especially to reduce unauthorized toll charges.

RESOURCE SECURITY

Since authorized use is controlled by a voice verification program, it is important to control the unauthorized access to computer resources such as files and applications outside of the voice verification program. In accordance with one embodiment, access to files and applications is controlled by encryption. While there are a variety of encryption techniques that may be usefully employed, such as RSA, DES (data encryption standard), public key encryption, reversible transformation (e.g. exclusive or) with a pseudo-random number stream, and character substitution tables, the present invention is not limited to any particular encryption technique. Encryption of files, whose decryption is performed if the voice verification is successful, provides an affordable protection strategy that is appropriate for

personal computers and laptops, especially when only some of the files on the computer are desired to be protected.

In some cases, it is important to conceal the name of a file from unauthorized users, because the existence and nature of the file may, by itself, constitute valuable information. Accordingly, one embodiment of the invention pertains to a "vault" in which all protected files and applications are stored. A vault may be implemented by a directory in the file system, in which the name of every file therein is scrambled. Consequently, a user must first be verified to know which files have been placed in the vault.

FIG. 6A illustrates a main application window 600 that is started after a successful user authentication. The main application is responsible for managing a plurality of files, including executable files for applications, especially by encrypting and decrypting files and moving encrypted files into and out of the vault. The main application window 600 displays a list of files 602 that are being managed. Management information is associated with each file, such as the original path (or directory) 604 of the file, the original name 606 of the file, and the status 608 of the file. This management information is preferably stored in a file block at the end of an encrypted file and also separately in dynamic memory when the voice verification management program is running. The management information for unencrypted or decrypted files is only stored separately from the files such as in dynamic memory; thus, unencrypted files are no longer managed by the system when the main application exits.

FIG. 6B illustrates a file menu 610 containing file management commands that are found in one implemention. The file menu 610 includes collection commands 612 for adding and removing files from the current collection 602. Encryption commands 614 are also found on the file menu. These encryption commands 614 allow the user to encrypt and decrypt files and move encrypted files into and out of the vault. A drag-and-drop interface may also be used to add and encrypt files (and vice versa).

FIG. 7 shows steps involved with encrypting files under management of a voice verification file management program. At step 702, a selected file is encrypted by a desired encryption technique. After the file is encrypted, management information about the file, such as the original path and name, is collected and appended into a file block that is allocated at the end of the file. Furthermore, the extension of the file is renamed in step 704, so that outside programs such as MICROSOFT WINDOWS EXPLORER™ can recognize that the file is encrypted and useless without the voice verification application. Preferably, the file extensions are registered in the system registry to indicate that the voice verification

application should be invoked when the encrypted file is doubled clicked or otherwise selected in EXPLORER™ or other file management programs.

Step 706 tests whether the user is requesting to put the file into the vault. This request may occur through a separate sub-menu item on the file menu 610 or through a checkbox or other user input on a dialog box. If the file is requested to be put into the vault, execution proceeds to step 708 where the file is copied into the vault directory. At step 710, the file name is scrambled, for example, by assigning the file an index number and converting the number into printable alphanumeric characters.

At step 712, the file is checked to see if it is an executable file for a computer application. If the file is an executable file, then a front-end voice verification program is copied into the original name of the executable (step 714). The front-end voice verification program is configured, when executed, to receive and verify an input voice sample as belonging to an enrolled user. If verified, then the corresponding encrypted application, which name differs only in the extension, such as "vexe", is decrypted and launched.

One reason for the different treatment of data files and executable is to preserve a consistent double-click interface for using an encrypted file, even in a standard program such as EXPLORER™. Although an encrypted application file is no longer executable, the front-end voice verification program is, so that double-clicking on what appears to be an executable file still seamlessly works.

Referring back to FIG. 6B, another option in group 614 on the file menu 610 is to decrypt files that have been encrypted. FIG. 8 is a flowchart showing steps involved in decrypting a file under management of a voice verification file management program. In step 802, the file is decrypted. If the file was originally an executable file, determined by examining the extension of the file (if "vexe") or checking the file data block of file management information (step 804), then the front-end voice verification program is deleted (step 806). Execution resumes at step 808, where the file extension is renamed back to the original. If the file was in the vault (tested at step 810), additional processing occurs by copying the file to its original directory (step 812) and the name of the file is renamed back to the original name (step 814). The information to perform these actions was stored in a file data block within the encrypted file.

Referring yet again to FIG. 6B, another group 616 of operations relate to importing and exporting encrypted files, so that another user of the voice verification file management can use files that were encrypted for one user. As illustrated in FIG. 6C, an export files

encryption key dialog box 620 is presented wherein the exporting user can specify an optional encryption key 622 or activate a button 624 to export with no additional key.

FIG. 9A depicts a user menu 900 that includes an entry for logging off, an entry 902 for obtaining a one-time password, and an entry for changing the user profile 904. One of dialog boxes displayed for changing the user profile 904 is a re-enrollment dialog box 910 in FIG. 9B, which allows to user to re-enter voice samples. The a re-enrollment dialog box 910 also provides a test button 914 to test how well the user's utterances are matched, and a threshold slider 916 for adjusting the threshold setting used for determining a match between more tolerant and more secure. FIG. 9C shows an exemplary dialog box 920 that displays a new one-time password 922 that is only valid for a single use.

While this invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not limited to the disclosed embodiment, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

WHAT IS CLAIMED IS:

1. A method for controlling access to a file, comprising:
receiving an input voice sample from a user;
verifying that the input voice sample belongs to an enrolled user; and
decrypting the file based on a result of said verifying.

2. The method of claim 1, further comprising prompting the user to speak the user's name before receiving the input voice sample.

3. The method of claim 1, further comprising prompting the user to speak a predetermined word before receiving the input voice sample.

4. The method of claim 1, wherein verifying that the input voice sample belongs to an enrolled user includes:
extracting an input voice print from the input voice sample; and
comparing the input voice print with an enrolled voice print extracted from a voice sample of the enrolled user to determine whether the input voice print matches the enrolled voice print.

5. The method of claim 4, wherein comparing the input voice print includes:
calculating a dissimilarity measure between the input voice print and the enrolled voice print; and
comparing the dissimilarity measure with a threshold value.

6. The method of claim 5, further comprising providing a slider bar in a user interface for setting the threshold value.

7. The method of claim 5, wherein calculating the dissimilarity measure includes calculating a cost of a path with a minimum sum of Euclidean distances.

8. The method of claim 4, wherein extracting the input voice print from the input voice sample includes:

segmenting the input voice sample into a plurality of frames; and

calculating a plurality of Cepstral coefficients for each of the frames.

9. The method of claim 4, further comprising:

receiving an enrolled voice sample from the enrolled user; an

extracting the enrolled voice print from the enrolled voice sample.

10. The method of claim 9, further comprising:

receiving a second enrolled voice sample from the enrolled user; and

updating the enrolled voice print by extracting a second enrolled voice print from the second enrolled voice sample.

11. The method of claim 1, further comprising:

prompting the user to answer a personal question;

receiving a response from the user to the personal question;

comparing the response with an enrolled response; and

decrypting the file further based on a result of comparing the response.

12. The method of claim 11, further comprising selecting the personal question from a plurality a predetermined personal questions about a color of a car, a make of the car, a name of an elementary school, a name of a seventh grade school, a father's birth place, a mother's birth place, a mother's maiden name, and a last number of social security number digits.

13. The method of claim 1, further comprising:

generating a single use password;

displaying the single use password;

receiving input of the single use password from the user; and

decrypting the file further based on said receiving the input of the single use password.

14. A method of controlling access to a plurality of files, comprising:

receiving an input voice sample from a user;

verifying that the input voice sample belongs to an enrolled user; and
if the input voice sample is verified as belonging to the enrolled user, then presenting a user interface for providing the user access to the files.

15. The method of claim 14, wherein presenting the user interface includes:
displaying names of the files;
receiving a selection for one of the files; and
decrypting the one of the files.

16. The method of claim 15, further comprising scrambling the names of the files as stored in a file system.

17. The method of claim 14, wherein presenting the user interface includes:
displaying names of the files;
receiving a selection for one of the files; and
decrypting the one of the files.

18. The method of claim 14, further comprising storing the files in a read-only memory.

19. The method of claim 14, further comprising exporting one of the files in an encrypted format.

20. A method for controlling access to a computer application, comprising:
receiving an input voice sample from a user;
verifying that the input voice sample belongs to an enrolled user; and
launching the application based on a result of said verifying.

21. The method of claim 20, further comprising:
renaming an executable application file of the computer application from an original name to a new name; and
storing an executable front-end file with the original name of the executable application file, said executable front-end file including instructions arranged to perform said steps of receiving, verifying, and launching.

22. The method of claim 20, wherein launching the application includes:
decrypting an encrypted executable file of the computer application to produce a decrypted executable file; and
executing the decrypted executable file.

23. A method for controlling access to a computer system, comprising:
receiving an input voice sample from a user;
verifying that the input voice sample belongs to an enrolled user; and
granting access to the computer system based on a result of said verifying.

24. A method for controlling access to a public telephone system, comprising:
receiving an input voice sample from a user over a telephone connection to a private branch exchange;
verifying that the input voice sample belongs to an enrolled user; and
granting access to the public telephone system based on a result of said verifying.

25. A computer-readable medium bearing instructions for controlling access to a file, said instructions arranged, when executed by one or more processors, to cause the one or more processors to perform the steps of:
receiving an input voice sample from a user;
verifying that the input voice sample belongs to an enrolled user; and
decrypting the file based on a result of said verifying.

26. The computer-readable medium of claim 25, wherein said instructions are further arranged to cause the one or more processors to perform the step of prompting the user to speak the user's name before receiving the input voice sample.

27. The computer-readable medium of claim 25, wherein said instructions are further arranged to cause the one or more processors to perform the step of prompting the user to speak a predetermined word before receiving the input voice sample.

28. The computer-readable medium of claim 25, wherein verifying that the input voice sample belongs to an enrolled user includes:

extracting an input voice print

from the input voice sample; and

comparing the input voice print with an enrolled voice print extracted from a voice sample of the enrolled user to determine whether the input voice print matches the enrolled voice print.

29. The computer-readable medium of claim 28, wherein comparing the input voice print includes:

calculating a dissimilarity measure between the input voice print and the enrolled voice print; and

comparing the dissimilarity measure with a threshold value.

30. The computer-readable medium of claim 29, wherein said instructions are further arranged to cause the one or more processors to perform the step of providing a slider bar in a user interface for setting the threshold value.

31. The computer-readable medium of claim 29, wherein calculating the dissimilarity measure includes calculating a cost of a path with a minimum sum of Euclidean distances.

32. The computer-readable medium of claim 28, wherein extracting the input voice print from the input voice sample includes:

segmenting the input voice sample into a plurality of frames; and

calculating a plurality of Cepstral coefficients for each of the frames.

33. The computer-readable medium of claim 28, wherein said instructions are further arranged to cause the one or more processors to perform the steps of:

receiving an enrolled voice sample from the enrolled user; an

extracting the enrolled voice print from the enrolled voice sample.

34. The computer-readable medium of claim 33, wherein said instructions are further arranged to cause the one or more processors to perform the steps of:

receiving a second enrolled voice sample from the enrolled user; and

updating the enrolled voice print by extracting a second enrolled voice print from the second enrolled voice sample.

35. The computer-readable medium of claim 25, wherein said instructions are further arranged to cause the one or more processors to perform the steps of:

prompting the user to answer a personal question;

receiving a response from the user to the personal question;

comparing the response with an enrolled response; and

decrypting the file further based on a result of comparing the response.

36. The computer-readable medium of claim 35, wherein said instructions are further arranged to cause the one or more processors to perform the step of selecting the personal question from a plurality a predetermined personal questions about a color of a car, a make of the car, a name of an elementary school, a name of a seventh grade school, a father's birth place, a mother's birth place, a mother's maiden name, and a last number of social security number digits.

37. The computer-readable medium of claim 25, wherein said instructions are further arranged to cause the one or more processors to perform the steps of:

generating a single use password;

displaying the single use password;

receiving input of the single use password from the user; and

decrypting the file further based on said receiving the input of the single use password.

38. A computer-readable medium bearing instructions for controlling access to a plurality of files, said instructions arranged, when executed by one or more processors, to cause the one or more processors to perform the steps of:

receiving an input voice sample from a user;

verifying that the input voice sample belongs to an enrolled user; and

if the input voice sample is verified as belonging to the enrolled user, then presenting a user interface for providing the user access to the files.

39. The computer-readable medium of claim 38, wherein presenting the user interface includes:

displaying names of the files;

receiving a selection for one of the files; and

decrypting the one of the files.

40. The computer-readable medium of claim 39, wherein said instructions are further arranged to cause the one or more processors to perform the step of scrambling the names of the files as stored in a file system.

41. The computer-readable medium of claim 38, wherein presenting the user interface includes:

displaying names of the files;

receiving a selection for one of the files; and

decrypting the one of the files.

42. The computer-readable medium of claim 38, wherein said instructions are further arranged to cause the one or more processors to perform the step of storing the files in a read-only memory.

43. The computer-readable medium of claim 38, wherein said instructions are further arranged to cause the one or more processors to perform the step of exporting one of the files in an encrypted format.

44. A computer-readable medium bearing instructions for controlling access to a computer application, wherein said instructions are further arranged to cause the one or more processors to perform the steps of:

receiving an input voice sample from a user;

verifying that the input voice sample belongs to an enrolled user; and

launching the application based on a result of said verifying.

45. The computer-readable medium of claim 44, wherein said instructions are further arranged to cause the one or more processors to perform the steps of:

renaming an executable application file of the computer application from an original name to a new name; and

storing an executable front-end file with the original name of the executable application file, said executable front-end file including instructions arranged to perform said steps of receiving, verifying, and launching.

46. The computer-readable medium of claim 44, wherein launching the application includes:

decrypting an encrypted executable file of the computer application to produce a decrypted executable file; and

executing the decrypted executable file.

47. A computer system for controlling access to a file, comprising:

a microphone for receiving an input voice sample from a user;

a storage device for storing the file;

a processor coupled to microphone and storage device and configured to perform the steps of:

verifying that the input voice sample belongs to an enrolled user; and

decrypting the file based on a result of said verifying.

48. A computer system for controlling access to a plurality of files, comprising:

a microphone for receiving an input voice sample from a user;

a storage device for storing the files;

a processor coupled to microphone and storage device and configured to perform the steps of:

verifying that the input voice sample belongs to an enrolled user; and

if the input voice sample is verified as belonging to the enrolled user, then presenting a user interface for providing the user access to the files.

49. A computer system for controlling access to a computer application, comprising:

a microphone for receiving an input voice sample from a user;

a storage device for storing the computer application;

a processor coupled to microphone and storage device and configured to perform the steps of:

verifying that the input voice sample belongs to an enrolled user; and

launching the application based on a result of said verifying.

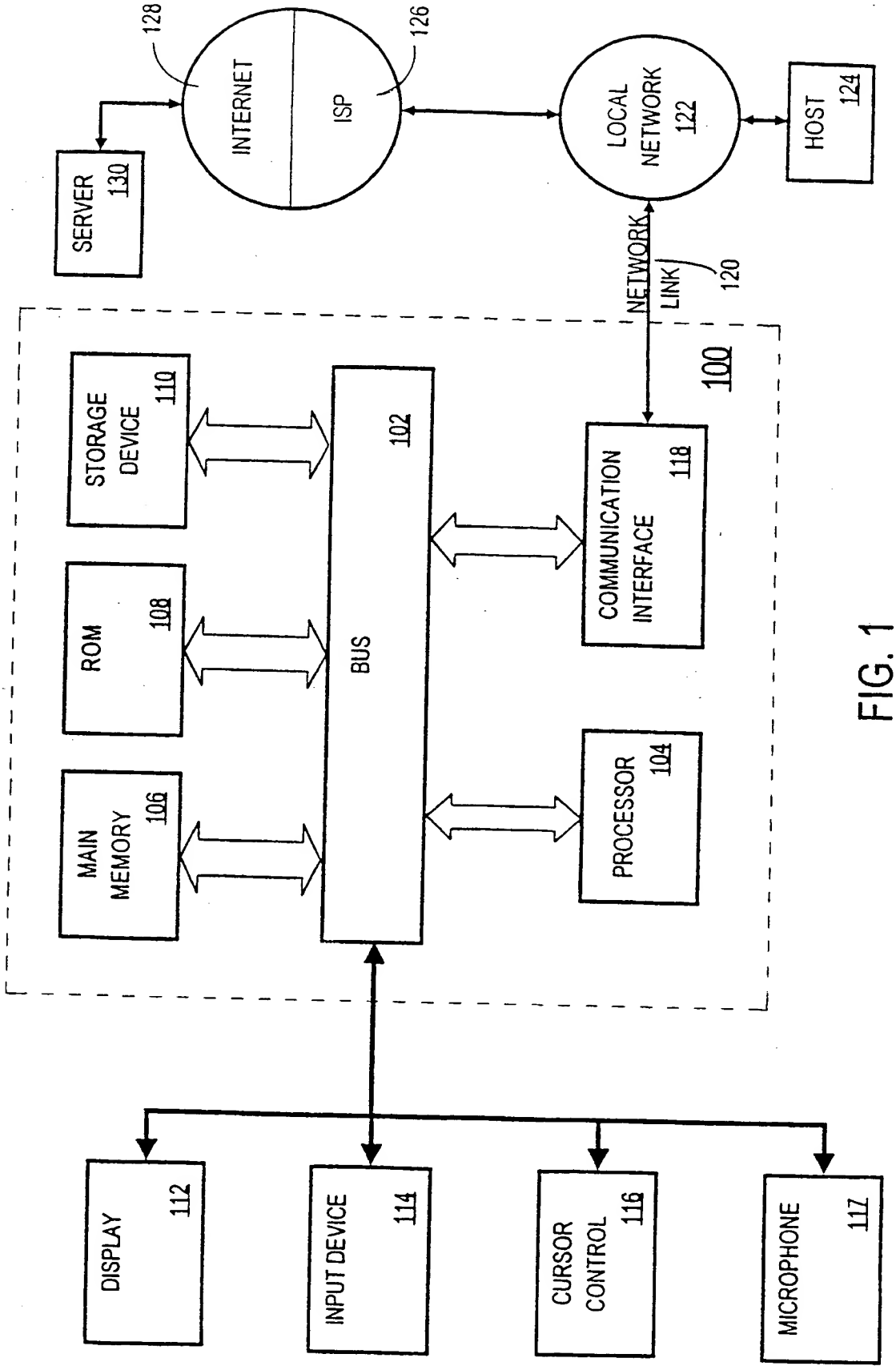


FIG. 1

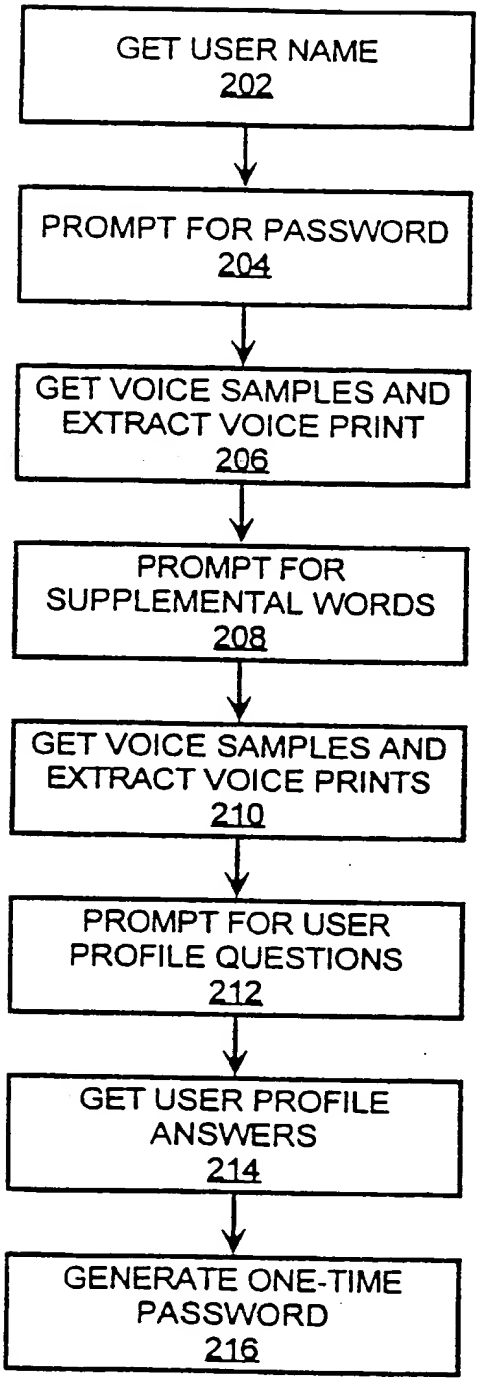


FIG. 2

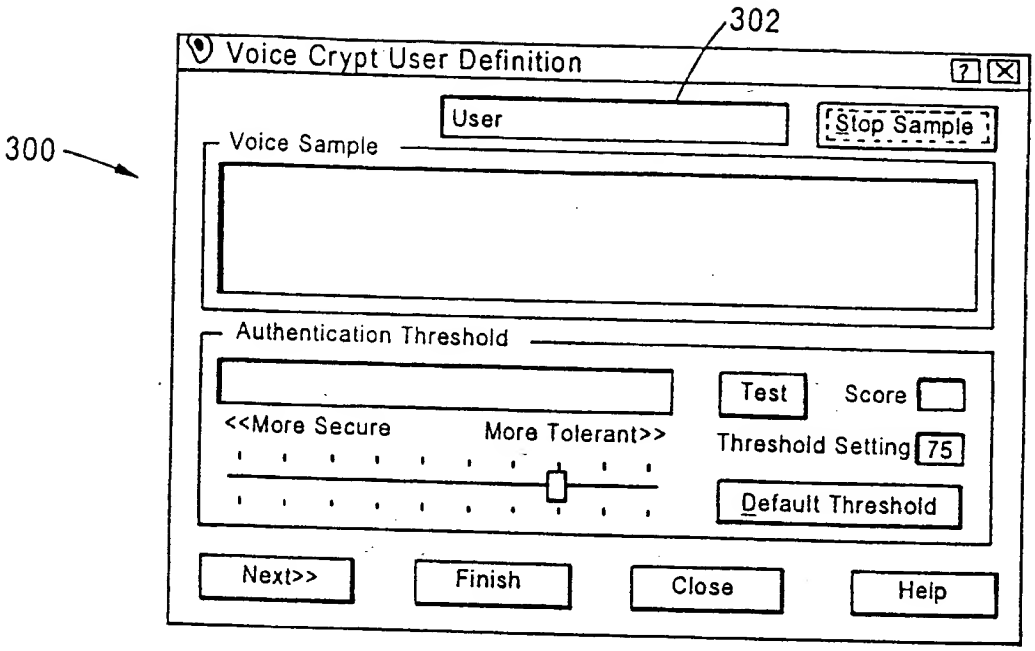


FIG. 3A

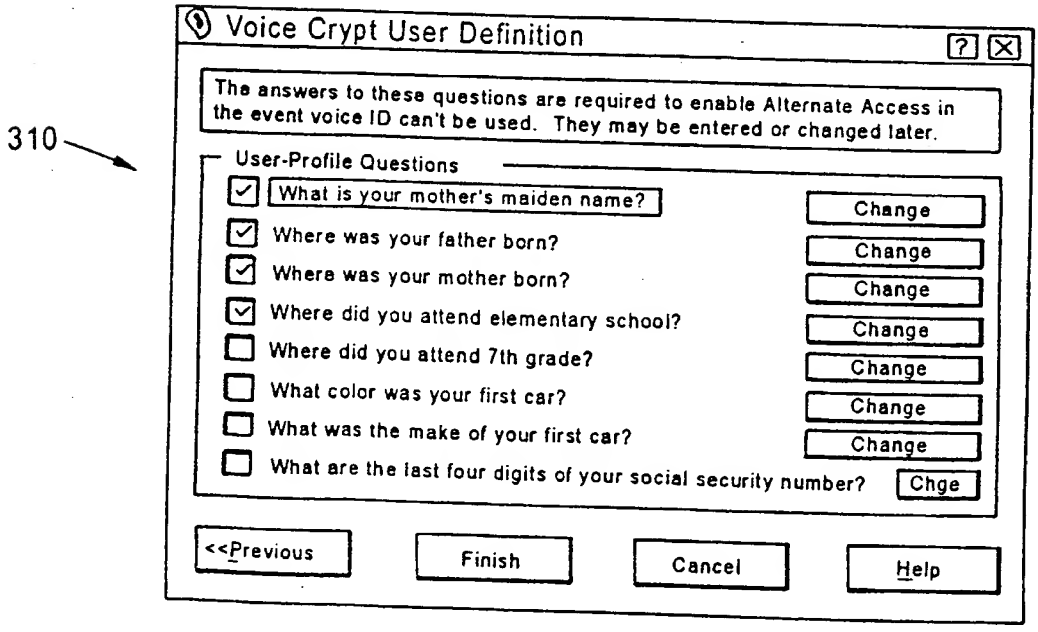


FIG. 3B

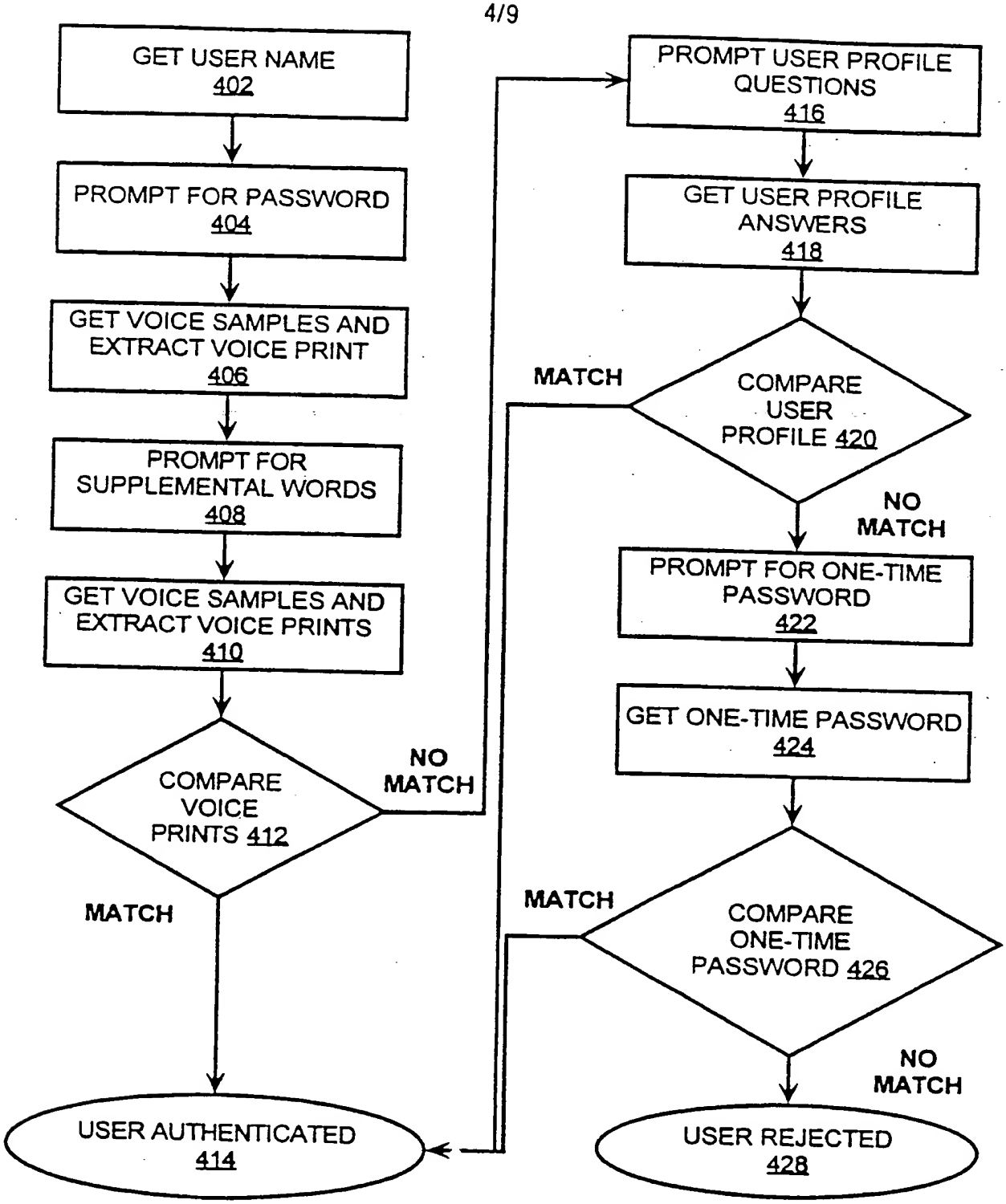


FIG. 4

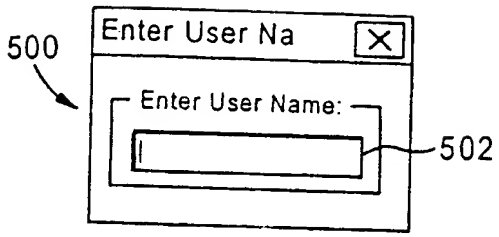


FIG. 5A

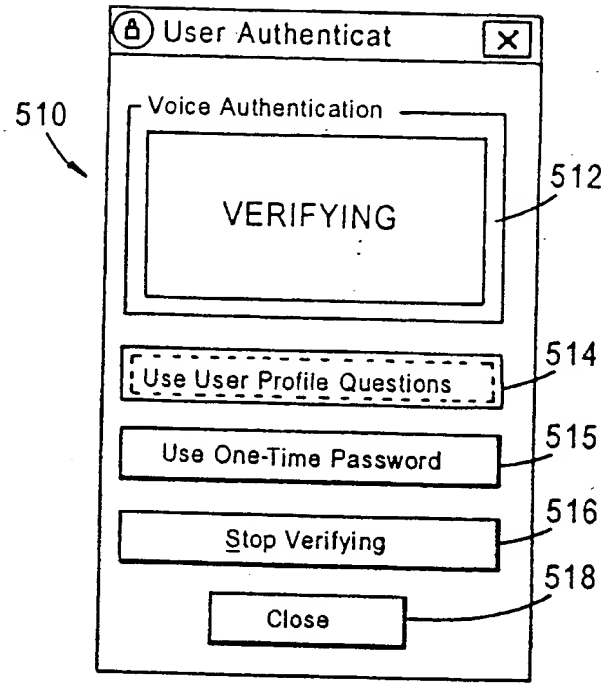


FIG. 5B

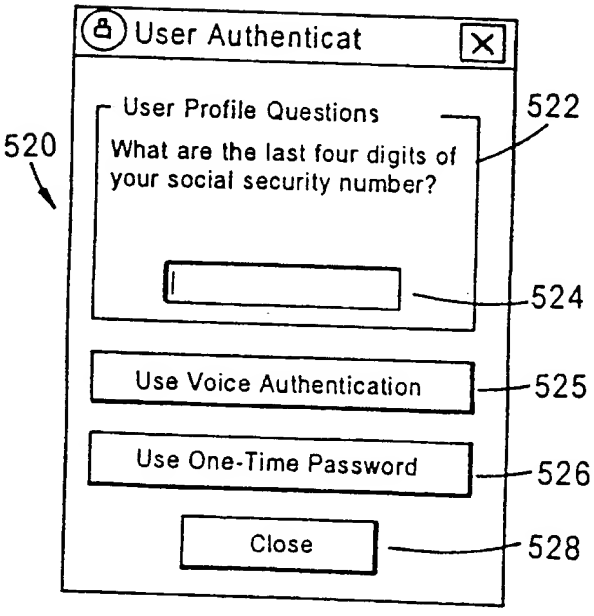


FIG. 5C

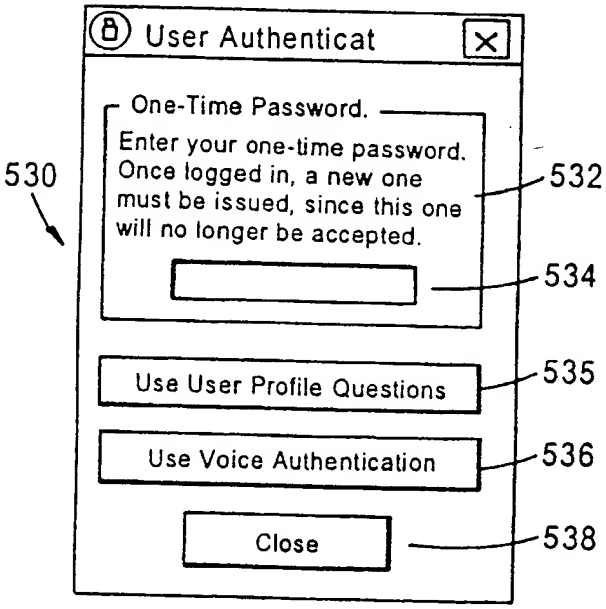


FIG. 5D

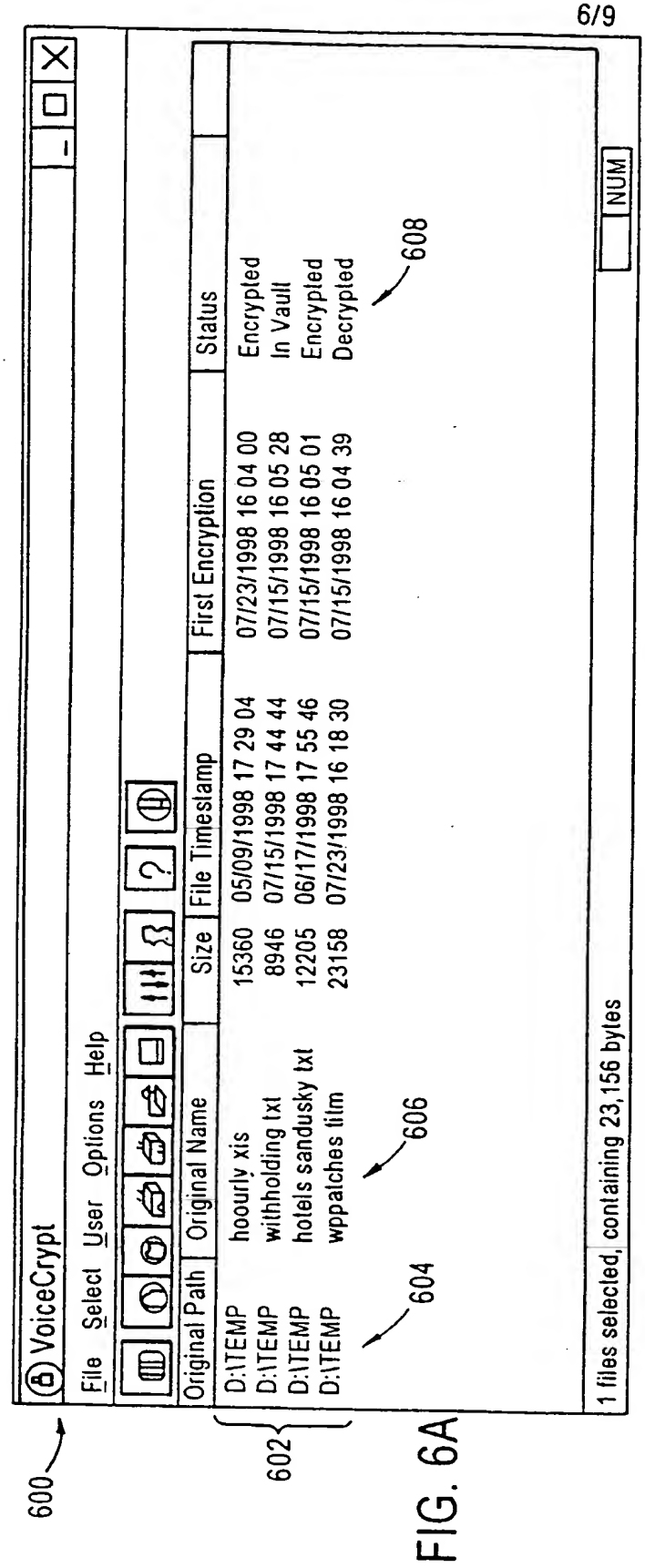


FIG. 6A

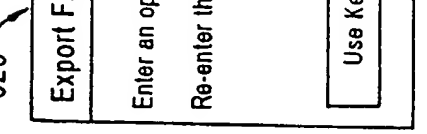


FIG. 6B

FIG. 6C

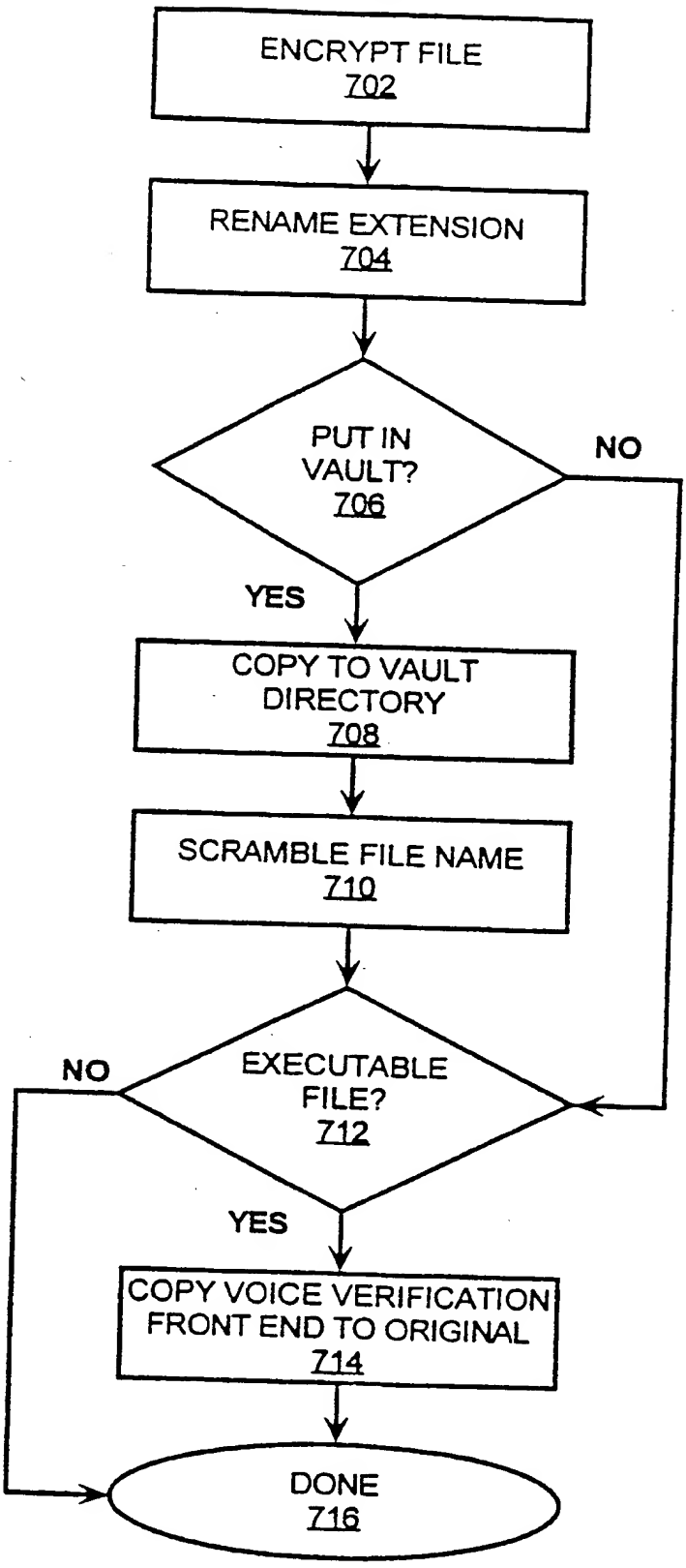


FIG. 7

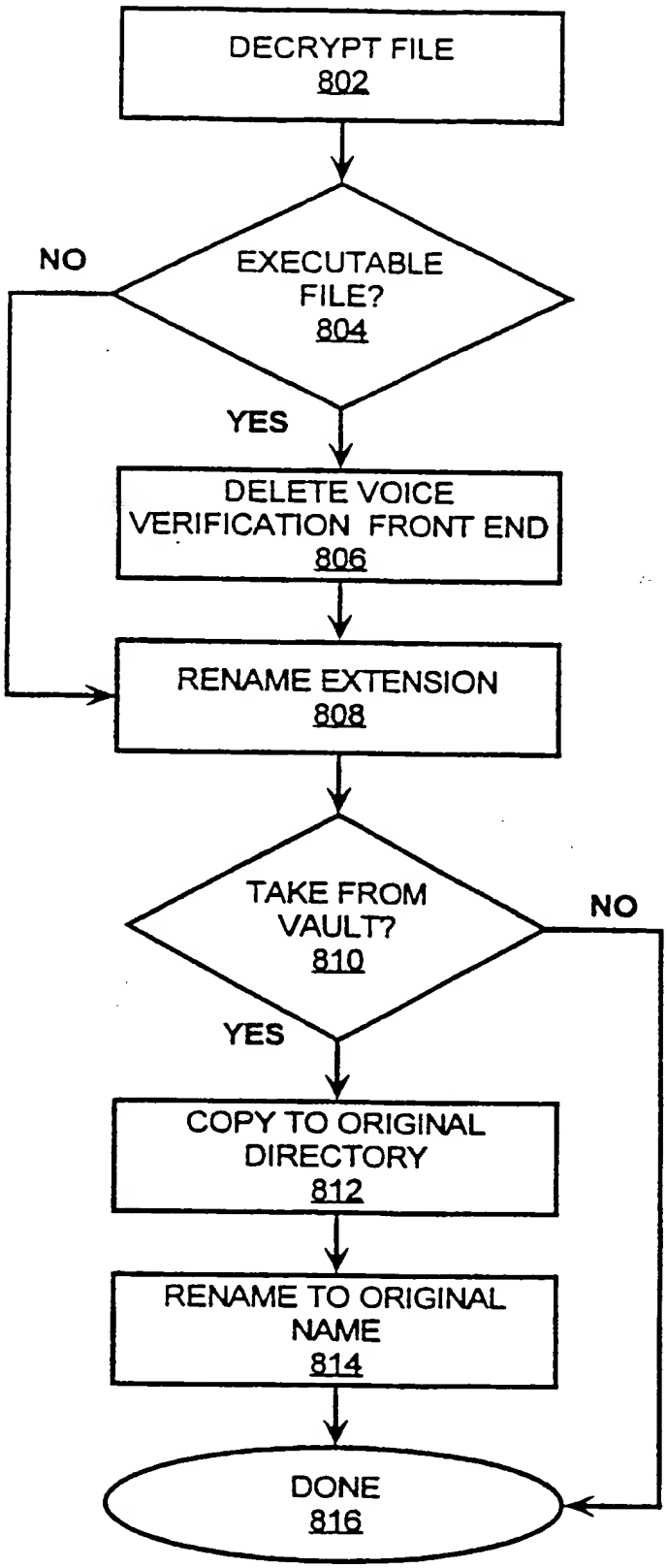


FIG. 8

FIG. 9A

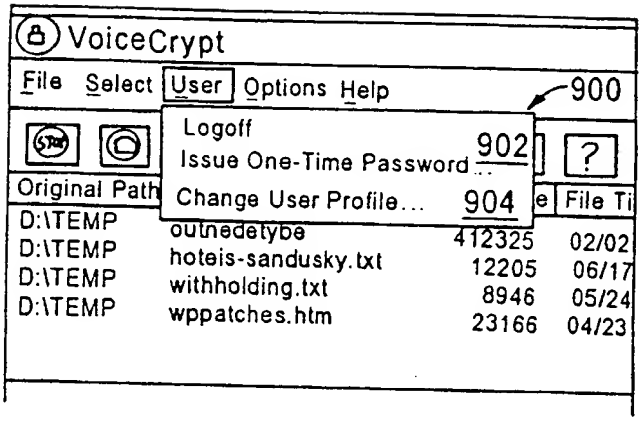


FIG. 9B

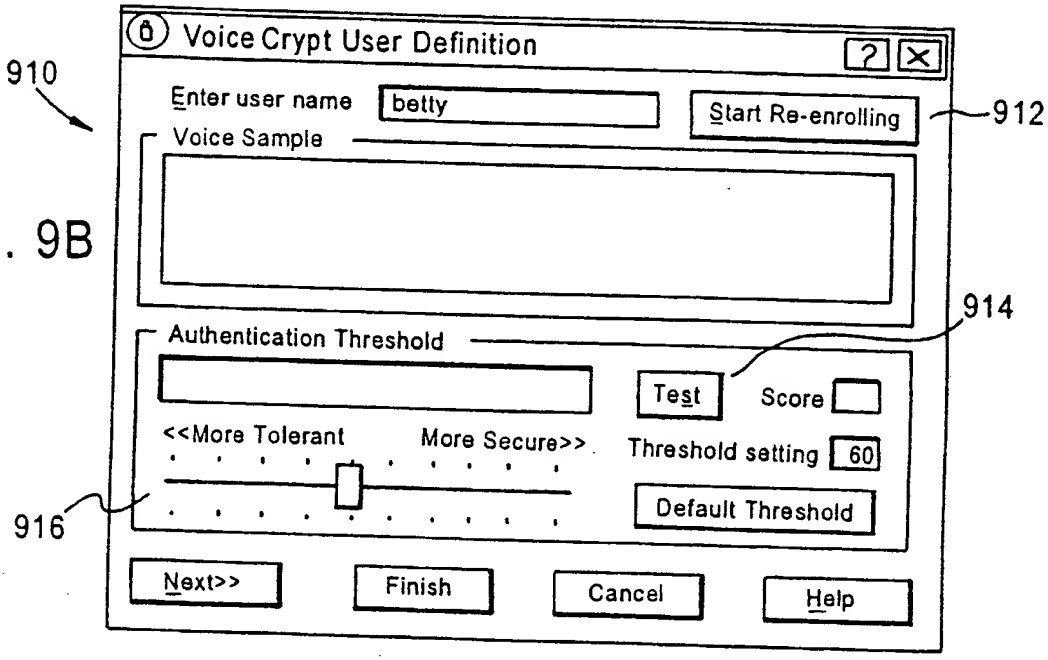
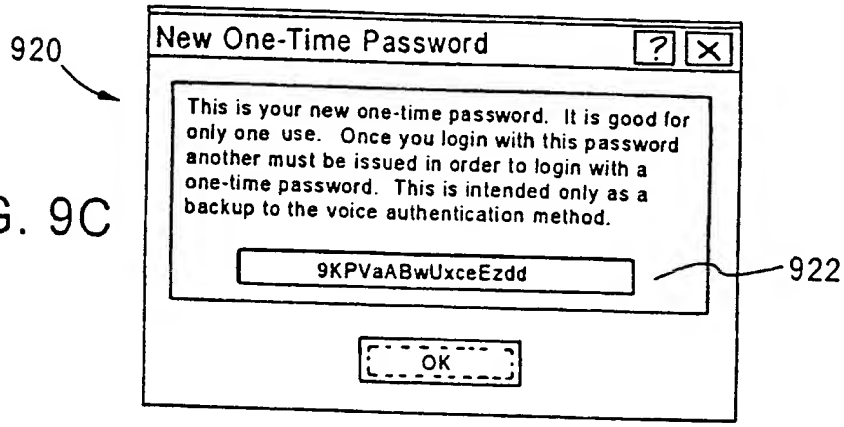


FIG. 9C



INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/16880

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F3/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G10L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SCHALK T B: "SPEAKER VERIFICATION OVER THE TELEPHONE NETWORK" SPEECH TECHNOLOGY. MAN-MACHINE VOICE COMMUNICATIONS, vol. 5, no. 3, 1 February 1991 (1991-02-01), pages 32-35, XP000207992 ISSN: 0744-1355 * Paragraph "VVS Technology" *	14,23, 24,38,48
Y	idem	1-5, 7-11,13, 15-22, 25-29, 31-37, 39-47,49

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 October 1999	27/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Krembel, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/16880

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 751 814 A (KAFRI ODED) 12 May 1998 (1998-05-12) column 3, line 17 - line 32	1-6, 8-11,13, 15-22, 25-37, 39-47,49
Y	FURUI S: "CEPSTRAL ANALYSIS TECHNIQUE FOR AUTOMATIC SPEAKER VERIFICATION" IEEE TRANSACTIONS ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING, vol. ASSP-29, no. 2, 1 April 1981 (1981-04-01), pages 254-272, XP002020822 abstract	4-10, 29-34
Y	"Enrollment options" IBM VOICE TYPE ONLINE GUIDE : SPEECH.INF, 'Disk! 1993, XP002118361 Help File * Section : "Match between word and sound" *	6,30

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

ormation on patent family members

International Application No
PCT/US 99/16880

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5751814 A	12-05-1998	IL 114361 A	16-08-1998